UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,882	10/28/2003	Jae Deok Lim	P69238US0	4036

22429 7590 04/30/2008
LOWE HAUPTMAN HAM & BERNER, LLP
1700 DIAGONAL ROAD
SUITE 300
ALEXANDRIA, VA 22314

EXAMINER	
SANDOVAL, KRISTIN D	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/693,882	Applicant(s) LIM ET AL.	
	Examiner KRISTIN D. SANDOVAL	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) *1-3 and 5-8* is/are allowed.

6)☒ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3 and 5-8 are pending.

Response to Arguments

2. Applicant's arguments filed February 4, 2008 have been fully considered but they are not persuasive.

Applicant argues that the prior art cited fails to teach applying a trusted header without user manipulation when a destination node is a secure OS to which a MAC is applied and the user has a security class. The examiner respectfully disagrees. The trusted header is applied when the tunnel is being formed between secure OS's, thus he trusted header is applied to the packet without user manipulation as taught by Fiveash (3:17-18) and it's applied when the destination is a secure OS (Meyer, 2:65) to which a MAC is applied with a security class (Meyer, 6:20-25). Therefore, the prior art cited shows a trusted header being applied without user manipulation when a destination node is a secure OS to which a MAC is applied and has a security class.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claim 1, as amended, is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,076,168 to William Alton Fiveash et al (hereinafter "Fiveash") in view of U.S. Patent 5,937,159 to William J. Meyers et al (hereinafter "Meyers"), further in view of S.

Kent, BBN Corp., "Security Architecture for the Internet Protocol, Request for Comments: 2401", November 1998, (hereinafter "RFC 2401").

Regarding (currently amended) claim 1, Fiveash discloses an apparatus for providing a trusted channel among operating systems to which a mandatory access control (MAC) policy is applied (column 2 lines 50-51 internet protocol security system), the apparatus comprising:

a data transmission side comprising:

a kernel memory (column 5 line 45 "kernel")

for specifying host addresses to which the trusted channel is to be applied (column 5 lines 43-47 "reading the description of the tunnel . . . and insert[ing] it into a kernel for use by IP traffic," the description includes the destination address) and

providing an encryption key for encryption of a packet (column 5 line 47 "encryption algorithm") and

an authentication key for generation of authentication data (column 5 lines 46-47 "authentication algorithm"); and

a trusted channel sub system (Figure 1 and column 2 lines 51-53 "an IP stack 110, a filter module 120, a tunnel module 130")

that determines, based upon MAC information from the MAC module and the host addresses to which a trusted channel is to be applied from the kernel memory, whether to apply the trusted channel, to user data to be transmitted to IP

layer (column 2 lines 58-60 “Filter module 120 and tunnel module 130 contain all the filter rules and tunnel definitions, respectively, used by the host system”);

creating a trusted channel header (column 3 lines 15-18 “If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network”);

encrypting a specific portion of the packet (column 1 lines 50-56 “When defining a tunnel, a user can choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used.”);

storing the authentication data in the trusted channel header (column 3 lines 15-18 “If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network); and

transmitting the packet through a network without user manipulation (column 3 lines 17-18 “it [the packet] is passed to the network”); and

[a] data reception side comprising:

a trusted channel sub system (column 2 lines 51-53 “an IP stack 110, a filter module 120, a tunnel module 130”)

operable to determine whether the trusted channel is applied (column 2 lines 63-66 "it is determined whether the data packet is encrypted and/or whether authentication is required. If so, the data packet is decrypted and/or authenticated");

to retrieve the authentication data in the trusted channel header (column 2 lines 65-66 "If [authentication is required], the data packet is . . . authenticated");

to decrypt the packet if the authentication data is valid (column 2 lines 63-67 and column 3 line 1 "If [the data packet is encrypted and/or authentication is required] the data packet is decrypted and/or authenticated . . . Then it is determined whether authentication or decryption of the packet has failed . . . If yes, the packet is dropped");

to conduct trusted channel header processings (column 3 lines 35-37 "Rules 2 and 3 are used to allow processing of AH and ESP headers, respectively"); and

to transfer the packet to an upper level by following a routine for delivering the packet to an input processing section of the upper level to thereby provide the packet to a user on the data reception side (column 3 lines 5-6 "the data packet is passed to the application layer"); and

a kernel memory configured to provide an authentication key to authenticate the packet and an encryption key to decrypt the packet (column 5 line 45 "kernel");

wherein the trusted channel header comprises authentication data operable to guarantee an integrity of the encrypted data (column 1 line 43 “authentication header”);

wherein the trusted header is applied without user manipulation when a destination node is an OS to which a MAC is applied, and the user has a security class, Fiveash (3:17-18) and it’s applied when the destination is a secure OS (Meyer, 2:65) to which a MAC is applied with a security class (Meyer, 6:20-25).

Fiveash does not explicitly disclose secure operating systems (OSs), a MAC module for providing MAC information of a user on a data transmission side, an initial vector for the decryption of the encrypted data, a next protocol field for a correct upper protocol processing, a header length for identifying a length of the header, a padding length for indicating a length of padding used for data encryption; and a MAC security class and a MAC category for delivering the MAC information of the user.

Meyers teaches a secure operating system (OS) (column 2 line 65). Meyers further teaches a MAC module for providing MAC information of a user on a data transmission side (column 6 lines 9-10 “MAC . . . controls a subject’s access to information and objects”). Meyers discloses a MAC security class and a MAC category for delivering the MAC information of the user (column 6 lines 20-25 “MAC label—a label placed on subjects . . . in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)”).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Fiveash with the secure operating systems and MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status (*see* Fiveash col. 1-2 ll. 57-6 and Meyers col. 2 ll. 5-8, 14-18 and 26-29).

Fiveash and Meyers fail to disclose an initial vector for the decryption of the encrypted data, a next protocol field for a correct upper protocol processing, a header length for identifying a length of the header, a padding length for indicating a length of padding used for data encryption.

RFC 2401 discloses an initial vector for the decryption of the encrypted data (page 15 paragraph 2 “IV,” being the standard abbreviation of initialization vector), a next protocol field for a correct upper protocol processing (page 18 paragraph 3 “IPv4 "Protocol" or the IPv6 "Next Header" fields”), and a header length for identifying a length of the header, (page 31 paragraph 10 “header length”); a padding length for indicating a length of padding used for data encryption (page 10-11 paragraphs 6-1 “padding also can be invoked”).

One skilled in the art at the time of the invention would have been motivated to refer to RFC 2401 to determine the standards for the state of the art in order to insure interoperability for security systems. Furthermore, it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Fiveash and Meyers with the protocol of RFC 2401 to insure interoperability for security systems (*see* RFC 2401, “2.1 Goals / Objectives / Requirements / Problem Description).

4. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Fiveash, Meyers and RFC 2401, and further in view of S. Kent, BBN Corp., "IP Encapsulating Security Payload (ESP), Request for Comments: 2406", November 1998, (hereinafter "RFC 2406").

Regarding (currently amended) claim 6, Fiveash discloses a method for providing a trusted channel among operating systems (OSs) (column 2 lines 50-51 internet protocol security system), including

a trusted channel sub system (Figure 1 and column 2 lines 51-53 "an IP stack 110, a filter module 120, a tunnel module 130"), a kernel memory on each of a data transmission side (column 5 lines 45 "kernel") and a data reception side (column 5 lines 30-32 "Both generated keys and specified keys are saved in the tunnel database") and

the method comprising the steps of:

(a) applying a trusted channel to a user provided packet to be transmitted to the IP layer, based upon the execution of a packet output routine of an Internet Protocol (IP) layer (column 2 lines 58-60 "Filter module 120 and tunnel module 130 contain all the filter rules and tunnel definitions, respectively, used by the host system") that searches the kernel memory on the data transmission side (column 5 lines 43-47 "tunnel database . . . reading the description of the tunnel . . . and insert[ing] it into a kernel for use by IP traffic," the description includes the destination address);

(b) creating a trusted channel header for storing a MAC security class and a MAC category of the user if the trusted channel is applied in step (a) (column 3 lines 15-

18 “If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network”);

(c) encrypting all areas of the trusted channel header excluding authentication data and an initial vector (column 1 lines 50-56 “When defining a tunnel, a user can choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used”);

generating authentication information for validating the packet (column 3 lines 15-18 “If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network”); and

storing the authentication information in the trusted channel header (column 3 lines 15-18 “If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network”);

(d) conducting a checksum processing (column 1 lines 40-41 “checksum function”) and a fragmentation processing (column 3 line 31 “Fragment_control”) of the packet and providing the packet to the trusted channel sub system on the data reception side through a network by following a lower level output routine (Figures 1 and 3 column 3 lines 10-11 and 17-18 “data packet is moved to the IP stack . . . it is passed to the network”);

(e) reassembling (column 3 line 31 "Fragment_control") and checksum processing (column 1 lines 40-41 "checksum function"), at a reception side IP input processing unit (column 3 lines 65-67 "defining the tunnel including associated filter rules on one end, creating a matching definition on the other end and activating the tunnel and filter rules on both ends") the packet received at the trusted channel sub system on the data reception side through the network and

(f) retrieving the authentication data in the trusted channel header before decrypting the packet if it is found in the step (e) that the trusted channel is applied to the packet (column 2 lines 63-66 "it is determined whether the data packet is encrypted and/or whether authentication is required. If so, the data packet is decrypted and/or authenticated"); and

decrypting the packet if the authentication data is valid while discarding the packet if the authentication data is not valid (column 2 lines 63-67 and column 3 line 1 "If [the data packet is encrypted and/or authentication is required] the data packet is decrypted and/or authenticated . . . Then it is determined whether authentication or decryption of the packet has failed . . . If yes, the packet is dropped"); and

(g) transferring the decrypted packet to an upper level by following a routine for delivering the packet to an input processing section of an upper level to thereby provide the packet to a user on the data reception side (column 3 lines 5-6 "the data packet is passed to the application layer");

Fiveash does not explicitly disclose secure operating systems (OSs), searching a MAC module, or the trusted channel header including a 128-bit authentication data field containing the authentication information for the encrypted packet, a 64-bit initial vector field used as encryption synchronization data of an encryption algorithm, a 8-bit next header field identifying an upper level protocol of IP, a 4-bit trusted channel header length filed indicating a length in bytes of the trusted channel header, a 4-bit padding length field designating a length in bytes of a padding used for the encryption of the packet, and a 16-bit MAC security class filed and a 64-bit MAC category field showing MAC information of the user who requests the communication.

Meyers teaches a secure operating system (OS) (column 2 line 65). Meyers further teaches a MAC module for providing MAC information of a user on a data transmission side (column 6 lines 9-10 “MAC . . . controls a subject’s access to information and objects”).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Fiveash with the secure operating systems and MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status (*see* Fiveash col. 1-2 ll. 57-6 and Meyers col. 2 ll. 5-8, 14-18 and 26-29).

Fiveash and Meyers do not explicitly disclose determining whether the trusted channel is applied to the packet by examining a next protocol field of an IP header in order to decrypt the packet. However, to do so is taught by RFC 2401 (page 33 paragraph 4 “Each inbound IP datagram to which IPsec processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field”).

One skilled in the art at the time of the invention would have been motivated to refer to RFC 2401 to determine the standards for the state of the art in order to insure interoperability for security systems. Furthermore, it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Fiveash and Meyers with the protocol of RFC 2401 to insure interoperability for security systems (*see* RFC 2401, "2.1 Goals / Objectives / Requirements / Problem Description).

Fiveash, Meyers, and RFC 2401 do not disclose a trusted channel header including a 128-bit authentication data field containing the authentication information for the encrypted packet, a 64-bit initial vector field used as encryption synchronization data of an encryption algorithm, a 8-bit next header field identifying an upper level protocol of IP, a 4-bit trusted channel header length field indicating a length in bytes of the trusted channel header, a 4-bit padding length field designating a length in bytes of a padding used for the encryption of the packet, and a 16-bit MAC class field and a 64-bit MAC category field showing MAC information of the user who requests the communication.

However, RFC 2406 teaches a secure packet format including an authentication field of variable length (page 7 paragraph 7), including an initialization vector in a variable-length payload field for encryption synchronization (page 5 paragraph 3), an 8-bit next header field identifying an upper layer protocol (page 7 paragraph 5), and an 8-bit pad length field indicating the number of pad bytes (page 7 paragraph 3).

Although RFC 2406 does not disclose a 4-bit trusted channel header length field, the pad length field being 4-bits, or a 16-bit MAC class field and a 64-bit MAC category field, it would be obvious to one skilled in the art at the time of the invention to use 4 bits of the 8-bit pad

length field as a trusted channel header length field because the pad length and next header fields are to be right aligned in a 4-byte word so that the authentication field is aligned on a 4-byte boundary (page 6 paragraph 1). Doing so would facilitate the receiver efficiently processing the packet.

Therefore, it would have been obvious to one skilled in the art at the time of the invention to split the pad length field between trusted channel header length and pad length fields to achieve more efficient packet processing.

The authentication field of RFC 2406 includes an integrity check value of varying length requiring specification of the comparison rules and processing steps for validation (page 7 paragraph 7). Additionally, one skilled in the art at the time of the invention would have known that packet headers may have additional fields added and segmented as desired.

Therefore, it would have been obvious to one skilled in the art at the time of the invention to specify the MAC class field and MAC category fields as part of the integrity check to validate that the user appearing to request the communication was indeed the sending user.

One skilled in the art at the time of the invention would have been motivated to refer to RFC 2406 to determine the standards for the state of the art in order to insure interoperability for security systems. Furthermore, it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Fiveash, Meyers and RFC 2401 with the header format of RFC 2406 in order to use header structure to accomplish end to end security (*see* RFC 2406, page 2 paragraph 1).

Repeated Claim Rejections

Claim Rejections - 35 USC § 103

5. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash and Meyers further in view of U.S. Patent 5,983,350 to Spence Minear et al (hereinafter "Minear").

Regarding **claim 2**, Fiveash discloses application of the trusted channel being determined upon data transmission, if two requirements are satisfied: (column 5 lines 26-27 "A minimum set of parameters are necessary to identify a tunnel"). Meyers discloses that the user should have a MAC security class (column 6 lines 21-25 "The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)").

Fiveash and Meyers do not disclose the packet's destination address corresponding to one of the host addresses to which the trusted channel is applied. Minear teaches a destination address of the packet corresponding to one of the host addresses to which the trusted channel is applied (column 4 lines 31-33 "the sending firewall uses the . . . Destination Address to select an appropriate Security Association").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the minimum parameters of Fiveash and MAC labels of Meyers with Minear's use of destination address to determine when a secure communication mode is necessary.

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash, Meyers and Minear further in view of RFC 2401.

Regarding **claim 3**, Fiveash, Meyers and Minear do not disclose application of the trusted channel being investigated, in case of data reception, by checking whether the next protocol field of the IP header of the packet represents the trusted channel header.

However, RFC 2401 discloses application of the trusted channel being investigated, in case of data reception, by checking whether the next protocol field of the IP header of the packet represents the trusted channel header (page 33 paragraph 4 "Each inbound IP datagram to which IPsec processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field").

Therefore, it would have been obvious to one skilled in the art at the time of the invention to combine the use of the next protocol field as taught by RFC 2401 with the teachings of the internet security protocol of Fiveash, Meyers and Minear in order to expedite proper packet processing.

7. **Claim 4 is cancelled.**

8. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash, and Meyers in view of RFC 2401, and further in view of RFC 2406.

Regarding **claim 5**, Fiveash discloses an encryption area of the packet for maintaining security of the packet is set to be all areas thereof excluding an IP header area, the authentication data area and the initial vector area, (column 1 lines 50-56 "When defining a tunnel, a user can

choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used").

9. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash in view of Meyers and further in view of RFC 2401.

Regarding **claim 7**, Fiveash discloses application of the trusted channel being determined by examining whether a destination address of the packet corresponds to one of the host addresses to which the trusted channel is applied (column 3 lines 26-27 "Destination_address").

Fiveash does not explicitly disclose the user having a MAC security class. Meyers teaches a MAC security class (column 6 line 20 "MAC label").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of configuring internet protocol security tunnels disclosed in Fiveash for use with the MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status.

Regarding **claim 8**, Fiveash does not disclose the trusted channel header being recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side of the fact that the trusted channel is applied to the packet.

RFC 2401 teaches the trusted channel header being recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side of the fact that the trusted channel is applied to the packet (page 33 paragraph 4 "Each inbound IP datagram to which IPsec

processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field").

Therefore, it would have been obvious to one skilled in the art at the time of the invention to combine the use of the next protocol field as taught by RFC 2401 with the internet security protocol of Fiveash and Meyers in order to assist the receiving user in identifying that a particular packet has had the security policy applied so that proper processing can occur expeditiously.

10. Claim 9 is cancelled.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KRISTIN D. SANDOVAL whose telephone number is (571)272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin D Sandoval
Examiner
Art Unit 2132

/K. D. S./
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132